FusionPointAI

Enterprise Banking Blockchain Infrastructure

Your Bank. Your Blockchain. Your Rules.

Use these topics to organize technical discovery and institutional review. Exact interfaces, behavior, and responsibilities are confirmed for the configured deployment.

Network and asset foundations

Begin with network identity, environment boundaries, consensus and validator responsibilities, and native asset purpose. Confirm immutable identifiers and approval requirements before creation.

Network architecture

Identify components, boundaries, dependencies, participant roles, and the intended operating model. Record assumptions for technical discovery.

Environment separation

Describe production and non-production environments, access paths, data handling, and change promotion responsibilities.

Chain ID and network identity

Validate the Chain ID and other network identifiers before creation. Chain ID is immutable after creation.

Consensus and validator responsibilities

Document the consensus configuration, governance authority, and validation plan. Assign validator operation, maintenance, access, monitoring, and incident responsibilities to institutional or service roles.

Native asset configuration

Define asset purpose, naming, administrative controls, and transaction policy. Asset configuration does not establish reserve backing.

Reserve ownership and separation

The institution owns and manages its reserves. Keep reserve arrangements separate from FusionPointAI technology and service charges.

Controls, fees, and governance

Document the control authority, transaction policy, fee funding, and governance process as institution-owned decisions. Test the configured behavior before production.

Account, wallet, and operation restrictions

Specify restriction conditions for accounts, wallets, and operation types. Document authorized decision-makers, evidence, review and release procedures, and expected outcomes for permitted or denied activity.

Partial and full restrictions

Describe partial versus full restriction semantics, affected operations, authority, duration, and restoration process.

Administrative governance

Configure the administrator council, multi-approval threshold, proposal authority, execution permissions, and applicable delays. Changes remain auditable.

Democratic governance

Configure the DAO voting population, voting weights, proposal threshold, voting period, quorum, and execution process. Equal voting rights are not assumed.

Hybrid governance

Define how administrative and democratic approvals combine, including either-side or both-side authorization where configured. Record execution and timelock responsibilities.

Governed parameter changes

Classify mutable governed parameters, approval requirements, compatibility concerns, and coordinated upgrade procedures.

Transaction fees, gas, and sponsored-fee policies

Document the fee asset, payer, funding, and separation from service fees and reserves. Define eligible settlement assets and transactions, budgets, limits, approvals, monitoring, and exception procedures; eligibility is configuration-dependent.

Interfaces and institutional integration

Treat interfaces and integrations as deployment-specific. Confirm endpoint details, authentication, support, data ownership, and vendor dependencies before implementation.

Standard JSON-RPC reads

Standard read-only examples include eth_chainId, eth_blockNumber, and eth_getTransactionReceipt. Confirm actual endpoint behavior for the deployed network.

Transaction lifecycle

Map request, authorization, submission, confirmation observation, receipt handling, retries, and reconciliation responsibilities.

Explorer configuration

Define intended users, available information, branding requirements, access boundaries, hosting, updates, and support ownership.

Core banking integration

Assess system interfaces, data mapping, vendor dependencies, test access, security review, and implementation responsibilities.

SSO and IAM integration

Map identity sources, authentication expectations, roles, provisioning, access review, and deprovisioning. Custom assessment is required.

HSM and key management

Document key custody, HSM requirements, signing boundaries, access, rotation, recovery, and technical feasibility for custom integration.

SIEM, KYC, and compliance dependencies

Identify event sources, access controls, retention, alert ownership, and custom SIEM requirements. Describe institution-owned KYC or compliance workflows and data dependencies; no prebuilt integration or compliance outcome is implied.

Security, operations, and commercial delivery

Close discovery by confirming deployment, security, continuity, service responsibilities, and commercial terms. Record commitments only in approved contractual documents.

Access roles and approvals

Define privileged roles, separation of duties, approval paths, access review, emergency access, and audit evidence.

Deployment boundary

Agree hosting, connectivity, administrative control, location needs, dependencies, and the institution and service-provider responsibilities.

Capacity planning

Use workload discovery and architecture review to plan sizing. Do not infer throughput or service guarantees from indicative capacity descriptions.

Availability and resilience design

Document component dependencies, failure scenarios, recovery roles, and any agreed objectives. Contractual commitments must be explicit.

Disaster recovery

Define recovery scenarios, data and configuration restoration, exercise scope, responsibilities, and institution-approved objectives.

Security assessment scope

Agree assessment boundaries, evidence, deliverables, and responsibilities. An assessment is not a certification or audit opinion.

Operational support and reporting

Specify covered components, support channels, escalation, reporting sources, delivery format, and commercial terms in the agreement.

Migration and change management

Assess source state, migration dependencies, validation, cutover, rollback, versioning, approval, and coordinated upgrade procedures.

Pilot evaluation plan

Set evaluation objectives, duration, test scope, data boundaries, responsibilities, findings, and exit criteria. A pilot is not production service.

Pricing, quote, and production acceptance

Use current database pricing for indicative display. Production requires a formal quote and executed agreement; pilot credit is subject to stated eligibility and cap.

Pricing

Scope	Setup	Monthly	First year
Banking Blockchain Pilot	USD 15,000.00	USD 0.00	USD 15,000.00
Banking Core	USD 75,000.00	USD 15,000.00	USD 255,000.00
Banking Enterprise	USD 175,000.00	USD 30,000.00	USD 535,000.00
Banking Sovereign Starting at	USD 350,000.00	USD 50,000.00	USD 950,000.00

Pricing is prepared from the agreed scope and current database pricing. Production service requires a formal quote and executed agreement.